PART IV LOOKING FORWARD

The city, messy, anarchic, . . .
has been a place where those
without power get to execute a
project. They get to make history.
Saskia Sassen, 2013

TEN
HACK THE CITY

Over the course of the 1990s a new form of power emerged—one that reverberated on the global scale . . . and could be wielded by a scruffy teen in a basement. Film depictions like *The Matrix* and *Sneakers* dramatized cyber security and the power of connected computers as they became a very real force in the world. A new figure was cast: the hacker.

The notion of a hacker initially emerged in the domain of computer science, defined as "an expert at programming and solving problems with a computer; a person who illegally gains access to and sometimes tampers with information in a computer system."[1] Essentially a person who claims power in digital space, the hacker captured

public imagination as the world migrated online during the 1990s. Huge global networks were being built, and their (malicious) destabilization became an immediate possibility. Hackers' activity was wrapped in a shroud of mystique, surrounded by call signs, offshore teams, and infected USB drives.

Hacking into information systems, however, is nothing new—it goes hand in hand with the emergence of telecommunications. One of the first attacks struck Guglielmo Marconi's demonstration of radio transmission in 1903, when he communicated from Cornwall to London, three hundred miles away. Nevil Maskelyne—a music-hall magician and would-be wireless tycoon—had been frustrated by the Italian inventor's patents. In what was either an act of aggression or a demonstration of prowess, Maskelyne managed to take control of the system and broadcast obscene messages to the Royal Institution's scandalized audience.

With the spread of digitization during the twenty-first century, more and more systems can now be hacked. In the era of ubiquitous computing almost everything can be accessed, appropriated, and subverted—from computers to cars to washing machines. As the world goes online, it is becoming a hacker's playing field.[2]

The scope of "hack value" has simultaneously expanded—it is certainly more than creating malicious computer viruses. "It is hard to write a simple definition of something as varied as

hacking, but I think what these activities have in common is playfulness, cleverness, and exploration. Thus, hacking means exploring the limits of what is possible, in a spirit of playful cleverness. Activities that display playful cleverness have hack value."[3] Generally speaking, hackers are motivated by a challenge, and there are more and more challenges in hybridized digital and physical space.

The concept of "cleverness" is somewhat motive-agnostic, with connotations ranging widely, from innovative to sly to malicious. Although the tools and procedures of computer hacking are largely universal, the end results can be benign or malignant, creative or destructive. Two categories of hacker are generally identified as "white hat" and "black hat." The former is an ethical hacker who seeks to penetrate a computer system and identify its flaws in order to make it more secure. The latter is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain."[4] Black hat hackers have been codified as a new class of felon in US legislation, categorized as "cyber-criminals."

The 1990s saw a flurry of hacking activity on both sides of the white hat–black hat boundary. Cases spanned a wide spectrum, from cracking security systems to artificially winning a Porsche in a radio-show giveaway. Adrian Lamo became one of the most prominent figures in hacker culture, notoriously breaking into corporate systems such as Excite@Home, MCI WorldCom,

Yahoo, Microsoft, and Google. Most of the trespasses were magnanimous—Lamo subsequently contacted the companies, pointed out security flaws, and suggested fixes. His pseudo-legal activity finally caught up with him with a grand hack of the New York Times Company, where he uncovered the personal details of thousands of contributors to the paper, including celebrities and former presidents. To avoid jail time, he negotiated a plea bargain that included six months of house arrest.

Kevin Poulsen was a hacker from an early age. As a child, he learned how to whistle into a pay phone to connect a call for free, and over time his challenges incrementally grew in both risk and reward. Poulsen famously monopolized phone lines to ensure that he was the 102nd caller to a Los Angeles radio show and won a Porsche car. His career on the wrong side of the law climaxed in an extended chase with the FBI followed by fifty-one months of imprisonment. He was the first American ever to be sentenced with a ban on computer access after his release from prison (effective for three years).[5] After serving time, Poulsen doffed his black hat and became a senior editor at *Wired* magazine, focusing on cyber security.

Hacking is difficult to define, particularly because the boundary between malicious and magnanimous is blurry. The consistent and unifying feature is a common culture—one that very much predates the computer. Much of hacker culture originated on the MIT campus with the Tech Model Railroad Club. With

a stated passion for discovering the way things operate, mechanical and otherwise, the founding members shaped what would become hacking culture, codifying their ideas and vocabularies in the 1959 *Dictionary of the TMRC Language* (later a bible in geek lore). In this document they coined such phrases as "information wants to be free" and gave us the very term "hacker"—originally referring to someone who pulls off an elaborate college prank.

The club's first home was on the third floor of MIT Building 20, the "Plywood Palace," which was in many ways an incubator of early hacker aesthetic and ethos. The group was concerned with far more than model trains: they first subverted and reconfigured the room itself, as the history of the club makes clear: "Having space in a temporary building had the advantage that no one really cared what you did there, including altering the wiring or modifying the walls."[6] Building 20 was fertile ground for nearly limitless experimentation with both content and context, as it was for many other groups and researchers. The emerging aesthetic was ramshackle and ad hoc, but the building was a petri dish for (often anti-authoritarian) ingenuity.

There is a long history of appropriating and controlling physical space as a platform for ideological engagement, stretching far beyond the MIT campus. The city is a venue, and its plazas and squares can be loudspeakers. Because civic space is so often charged with a specific social, political, or religious identity, hacks in that space can be correspondingly incisive. Almost every revo-

lution has begun and ended in a public square: from Julius Caesar entering Rome to the 2014 protests in Ukraine. In the epochal moments of history, public actions subvert the intended use of the space or the ruling party that lays claim to it. The Place de la Concorde, the largest public square in Paris, was originally intended as a signifier of the monarch's power and was therefore a fitting site for the execution of Louis XVI. On January 21, 1793, at the culmination of the French Revolution, the king was beheaded, and the square was renamed Place de la Révolution. More than two hundred years later, Tahrir Square in Cairo saw mass participatory action by citizens that resulted in the downfall of Egyptian presidents Mubarak and Morsi in 2010 and 2013, respectively.

Civic action in physical space is not exclusively negative or revolutionary, nor must it be targeted at a specific leader. The city is simply a platform and an amplifier to be appropriated (or hacked) for any purpose. From the breadth and variety of uses—or hacks—throughout history, places acquire unique mythologies as aggregate residue. The National Mall in Washington, DC, one of the most visible spaces in the United States, has broadcast voices nationally and internationally: the "I Have a Dream" speech by Dr. Martin Luther King Jr. in 1963, the Vietnam War Moratorium Rally in 1969, a mass with Pope John Paul II in 1979, concerts by a wide variety of musicians, from the Beach Boys to Britney Spears, and the presidential inauguration every four years. While these events are not hacks in and of them-

People Congregated in Tahrir Square on February 9, 2011, by Jonathan Rashad

Ideas spread quickly online—social media, forums, and communication tools are all powerful media for community discussion, debate, and action. But physical urban space is, and will remain, the final stage. Revolutionary ideas and sentiments can spread like wildfire through online communities and spill into physical space, effectively challenging governments with unprecedented strength. A series of political demonstrations across the Arab world during 2011 have become known, collectively, as the Arab Spring. Strikes, marches, and protests were organized—and communicated to a rapt global audience—via social media platforms like Twitter and Flickr (the source of this photo). Pictured here is Tahrir Square, Cairo, during an event that has become emblematic of the movement. Through this demonstration, and series of similar ones, protestors contributed to the change of regimes in Egypt.

selves, they have a cultural weight that aggregates and lends gravity to future actions in the same space. Hacking the city in such a culturally charged site draws on the legacy of appropriations of civic space.

These events and actions prove the strength of urban hacking as a language of social statement. An iconic example by the artist and activist Oliviero Toscani, working for the Benetton group, radically challenged the Catholic culture of France and raised global awareness on World AIDS Day in 1993: the artist placed an enormous pink condom (seventy-two by eleven and one-half feet) on the obelisk in the Place de la Concorde. Given the immediate scrutiny of media outlets around the world, Toscani's act brought unprecedented media visibility to the disease, to social stigmatization, and to sexual health. In the same

Pink Condom by Oliviero Toscani for United Colors of Benetton, December 1, 1993

Public spaces can serve as tremendous platforms for social commentary. Cities are familiar—streets and squares and monuments belong to each and every resident—which lends power and gravity to urban subversions. As an undercover project for the 1993 World AIDS Day, the artist Oliviero Toscani installed a giant pink condom on the Luxor Obelisk at the Place de la Concorde, creating a shocking symbol of AIDS awareness in the center of Paris, at one of the city's most visible locations. Authorities intervened almost immediately, and the condom was removed the same day. Yet it captured the public imagination–since then, the hack has been repeated dozens of times, bringing a remarkable degree of visibility to the AIDS cause.

Paris, December 1st, 1993
World AIDS Day

city in 2014, ten thousand farmers protested European Union agricultural policy reforms by marching sheep through the streets, even taking them into the Louvre. The argument—that farmers do not make high-enough wages to take time to enjoy national treasures like the Louvre—was made blatantly clear as sheep flooded the museum's hallways. But even small hacks can make a sharp social critique, such as slightly altered signs in the London Underground that point out—and seek to improve—commuters' social habits by printing phrases like "Warning: do not make eye contact with fellow passengers."

The hack value of these instances is the connection between the particular space—its intended purpose and its history—and the revelatory transformation of the hack itself. Urban interventions would mean nothing without the physical settings they engage and without public scrutiny. If hacking is about understanding a system, appropriating it, and using it for alternate purposes, then the core of a truly successful hack in urban space involves, first, what the site means; second, how the hack appropriates the site; and third, how the hack transforms the site to communicate a message to a broad public.

Today, at the convergence of bits and atoms in urban space, there is a new dimension to hacking. Cities are increasingly suffused by a networked digital layer, and three important elements of hacker culture—computer geeks, protests, and social critiques—are powerfully colliding. What are the means, the

significance, and the potentials of hacking in tomorrow's smart cities? The digital and physical juncture will play host to—even amplify—the good, the bad, and the ugly of hacking.

The bad is already familiar. In the wake of notorious hackers like Lamo and Poulsen, the potential for destabilizing multinational systems through cyber terrorism has become a palpable threat—one that becomes yet more menacing as physical infrastructures are digitized. Metropolitan-scale systems such as subways and gas lines are immediately vulnerable to antagonistic infrastructural hacking.

Malicious weaponization of infrastructure systems has been a common subject of recent fiction and film. The threat resounds dramatically as a plot line precisely because it is uncomfortably close to reality. In 2010, Stuxnet, a powerful (and very real) malware, wiped out over one-fifth of Iran's nuclear centrifuge facilities. The virus targeted industrial-scale programmable logic controllers—the same kind of real-time control system drivers that are behind factory machinery, amusement parks, and digital light fixtures. Stuxnet came to life almost biologically: it self-propagated from machine to machine, it covered its tracks by sending all-clear messages from infected systems, and it lay dormant if its execution criteria were not met on a given machine. When active, the virus overrode the control system that governed a centrifuge's massive rotating components, causing the facility to violently tear itself apart. The elegance and

sophistication of the malware is often cited as incontrovertible evidence that major governments were on the playing field. Stuxnet took cyber-security specialists off guard. From their perspective: "We're all engineers here; we look at code. This was the first real threat we've seen where it had real-world political ramifications. That was something we had to come to terms with."[7]

Stuxnet proved the power of hacking at the juncture of digital and physical systems, and as the city becomes increasingly hybrid, the danger increases. The destructive potential of appropriating almost any smart system is proportionally threatening. Every dimension of the city could potentially be hacked: imagine careening autonomous vehicles, aggressively responsive architecture, or menacingly asynchronous energy distribution. A black hat hacker wields enormous power in cyber-physical space. In 2012, the US defense secretary, Leon Panetta, warned that the United States was vulnerable to a "cyber Pearl Harbor" that could, as a reporter paraphrased, "derail trains, poison water supplies, and cripple power grids."[8]

Hacking can serve an important positive function, however, both for social reasons and for security. The team at Kaspersky Lab that finally tracked down the Stuxnet virus (and its equally malicious progeny) in 2010 was a crack squad of former hackers and computer scientists experienced with tools and methods on both sides of the legal boundary. Such familiarity provides an

advantage in analyzing and diagnosing existing systems and in designing tighter security.

By exploiting loopholes and executing hacks, white hat hackers can discover vulnerabilities and point toward new standards, security protocols, or encryptions to increase safety. This is the potential of hacking as innovation. Just as the shabby—that is, hackable—MIT Building 20 was a hotbed of discovery, so, too could tomorrow's smart city spark creativity by incorporating a measure of hackability. Many people have advocated for more hackable cities in a variety of ways. Given a platform—the urban analogue of iOS or Android, for example—anyone and everyone could create city apps. One admittedly low-tech example is Parking Day, an opportunity for citizens across the country to appropriate parking spaces, design interventions, and suggest alternate futures for the enormous—and largely wasted—parking infrastructure. Since its inception in San Francisco in 2005, Parking Day has expanded across the globe through the use of digital platforms.

But this kind of initiative brings up an important consideration: the delicate balance between inspiring and pedantic. That is, if you make something hackable, have you neutered its hack value? If it is no longer a challenge, will it be hacked?

On the urban scale, an immediate answer is to open both platforms and data. Urban information would be fertile soil for innovation but nonetheless hands-off from a top-down perspec-

tive. Promoting openness could "activate additional elements of both knowledge practices and technological practices, generate more engagement by city residents, more cross-neighborhood comparisons, scale up to city level but from the ground up, lead to exchanges and collaborations, and on to a fully mobilized neighborhood and city culture." The city may become a complex mesh of transparent systems, where a rich trove of information promotes appropriation and experimentation. Access may come to be understood as a basic human right, what the philosopher Henri Lefebvre called "le droit à la ville," the right to the city. It is the demand for a "transformed and renewed access to urban life."[9]

Open data and platforms are nothing short of a key to sharing ideas, knowledge, and best practices with willing collaborators. "This would be but one step in a potentially much longer trajectory, one that might entail a re-making of the urban." Open data and platforms are as valuable to a smart, living city as accessible and open public space is to the traditional city. The processes of urbanization are "fundamentally political questions" that can only be realized between the top-down and bottom-up.[10] Open place–based application program interfaces (APIs) or data repositories may become new forums to spread ideas, to critique standard practices, or to express sociopolitical views.

Tools for opening cities will fulfill and make tangible a long-standing vision of urban co-creation, one that understands

"produced environments [as] specific historical results of socio-environmental processes." Futurecraft is one of the engines by which social processes can become spatial products. It is the mechanism that Lefebvre polemically called for in 1972. In essence: "The democratization of [the right to the city], and the construction of a broad social movement to enforce its will, is imperative if the dispossessed are to take back the control which they have for so long been denied, and if they are to institute new modes of urbanization. Lefebvre was right to insist that the revolution has to be urban, in the broadest sense of that term, or nothing at all."[11]

With increasingly ubiquitous computing, urban life plays out at the convergence of physical and digital space, and a new citizenship may emerge. Forums for participation may allow the citizenry to engage in collective action and transform the space around them: the city of the future will emerge from collaborative futurecraft at the intersection of the digital and physical worlds.

ELEVEN
EPILOGUE

Using the lens of futurecraft, we have considered some of the key forces at play in the city today—from energy to building, from transportation to knowledge sharing. Each of these ultimately weaves into a tapestry of citizen empowerment, suggesting the possibility of human participation in operating (and even hacking) the city. Top-down frameworks, the kinds of systems in large multinational corporations, are not enough; bottom-up actions are needed to transform urban spaces. There can be no smart city without smart citizens.

As the city becomes a forum for action and reaction, the playing field of urban innovation will continue to reach new communities. By necessity, every technology begins at

a particular place and time, and in many cases this is in research and development contexts in the industrially developed world. But from there it can expand in powerful and unpredictable ways. Twenty-five years ago, cell phones were exorbitantly expensive, a rarefied luxury for the global elite. Yet today, only a short time later, there are more active cell phones than there are human beings on the planet. In tandem with this diffusion are new opportunities for cell phones to serve as a tool of social empowerment.

Many of the technologies that are emerging in the developed world are likely to demonstrate their most potent impact in the entirely different contexts of emerging economies—where a myriad of challenges brought by urbanization will be decided in the decades to come. How might self-driving vehicles empower citizens and shape a new urban structure in countries that do not already have a robust public transportation network? How might digitally enhanced delivery networks help communities transform logistics in informal settlements? Across every sector, technological "leapfrogging" is becoming an increasingly important force in the world today.

Public engagement is a critical factor in discussions of our collective urban future. The vignettes and future scenarios throughout this book are not intended as predictions. They are ideas for debate, and we hope they will generate a critical conversation that could orient how we collectively think about

transforming the present. How these technologies play out will depend on our own actions and reactions.

This book will be successful if it achieves the goal of sparking informed discussions. We do not intend it to be an agenda but a framework for actions that may have a transformative impact on cities worldwide. In the words of Buckminster Fuller: "We are called to be the architects of the future, not its victims."